*Please note: This is a working draft of Directive 660.00. This is proposed language and the Bureau has not implemented any changes at this time. This is a new directive.

660.00 Management of Criminal Intelligence Files
1st Universal Review: 10/1/18 – ~~10/31/18~~ 11/9/18

Refer:

- 28 CFR § Part 23, Operating Policies
- ORS § 181A.250, Specific information not to be collected or maintained
- City of Portland Human Resources Administrative Rule 11.04, Protection of Restricted and Confidential Information
- City of Portland Records Retention Schedule 8011, Intelligence
- DIR 310.70, Dissemination of Information
- DIR 344.05, Bias-Based Policing/Policing Prohibited
- DIR 614.50, Release of Information
- DIR 631.30, Cooperation with Other Agencies

Definitions:

- Criminal Intelligence File: A collection of information about a person or group reasonably suspected to be currently or previously involved in criminal activity, which has been analyzed and utilized for purposes including, but not limited to: drawing comparisons between the person or group and other persons or groups similarly reasonably suspected of criminal activity; linking the person or group to other persons or groups similarly reasonably suspected of criminal activity; establishing the person's or groups' associations; providing safety information to officers on patrol; or creating an informational law enforcement bulletin.

- Criminal Intelligence System: Any formal or informal records system (database, application, physical equipment) that collects, stores, and disseminates investigative material found in a criminal intelligence file.

- Information: Data such as personally identifiable information as well as any known history and public records used to identify an individual or organization.

- Intelligence: The gathering and analysis of information which has been validated through various police reports, files, records, systems, and databases that establish a link between an individual and/or organization to criminal activity.

Policy:

1. This policy establishes the guidelines for the Portland Police Bureau (PPB) management of criminal intelligence files relating to individuals and/or organizations suspected of conducting or engaging in criminal conduct or activity. The Bureau comports with federal and state regulations regarding the collection of investigative material. Moving forward, any criminal intelligence file created after the enactment of this directive must adhere to the procedures set forth below.

2. Information gathering is a fundamental duty of law enforcement. The Bureau maintains a variety of basic information (e.g., reports, files, and databases that contain investigative or management information, public record information, commercial databases, and other fact-

based information) that is not subject to criminal intelligence system regulations. Members must be able to distinguish between basic information and criminal intelligence, which is subject to specific rules and regulations. Members should consult with a supervisor, the Bureau's Criminal Intelligence Unit (CIU), or the City Attorney's Office (CAO) if questions about the distinction exist.

3. PPB recognizes the significance and impact of collecting, gathering, creating, maintaining, and disseminating criminal intelligence files related to people and organizations. The Bureau expects its members to appropriately manage and safeguard any investigative material in order to preserve the privacy and constitutional rights afforded to individuals. Unauthorized uses of criminal intelligence files shall be investigated and may subject the member to disciplinary action.

Procedure:

1. In accordance with ORS § 181A.250, members shall not collect or maintain information about the political, religious, or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

2. Creation and Maintenance of Criminal Intelligence Files.
   - 2.1. Members must be able to articulate reasonable suspicion to collect, gather, and maintain intelligence on the subject(s) or enterprise(s) involved or potentially involved in criminal activity or activity that supports criminal conduct.
     - 2.1.1. Members may consult with a supervisor, CIU, or CAO prior to creating or maintaining a criminal intelligence file.
     - 2.1.2. Any Responsibility Unit (RU) that determines the necessity to maintain files not tied to a specific criminal case must have a Standard Operating Procedure (SOP) in place and approval from their overseeing Assistant Chief (AC) detailing the criteria for their creation and maintenance.
   - 2.2. Members shall not create criminal intelligence files related to individuals or enterprises without first establishing reasonable suspicion that definable criminal conduct or criminal activity is occurring, or has occurred, or is about to occur.
     - 2.2.1. Members shall review incoming and known information for relevancy, evaluate source reliability, and ensure the information is valid prior to inclusion in a criminal intelligence file.
     - 2.2.2. Members shall include a date and time stamp on all products (documents, spreadsheets, etc.) within a criminal intelligence file (printed or electronic) for retention, purging, and auditing purposes.
   - 2.3. Members may include in a criminal intelligence file names of individuals or organizations that are not suspected of criminal involvement so long as the information is clearly labeled as "noncriminal identifying information" and is otherwise relevant to the investigation of a specific individual or organization. Noncriminal identifying

information provides Bureau members with context regarding the criminal subject or criminal activity being investigated.

2.3.1. The "noncriminal identifying information" label may be removed if the non-suspect individual or organization becomes reasonably suspected of criminal activity.

2.4. Intelligence stored in a criminal intelligence system shall be reviewed at a minimum on a monthly basis by a supervisor to ensure the data is valid, accurate, relevant, and current.

3. Dissemination.

3.1. Members shall obtain a supervisor's approval prior to posting or disseminating criminal intelligence files.

3.2. Members shall not disseminate criminal intelligence files to external law enforcement agencies without prior consent from a supervisor or manager.

3.3. If the PPB Records Division contacts a member to obtain a criminal intelligence file, the member may provide the requested documents to the Records Division. However, members in the Records Division shall note any confidentiality or privacy concerns identified by the member providing the information.

4. Retention and Purging.

4.1. Any criminal intelligence document or file created by members for law enforcement purposes are subject to public records requests and must be maintained in accordance with federal and state regulations. In the case of most criminal intelligence documents or files, this timeframe will be five years, pursuant to Bureau of Justice Assistance (BJA) 28 CFR Part 23. Members may consult with the City Attorney's Office (CAO) for information regarding retention schedules.

4.2. Any criminal intelligence document or file that is no longer needed for an active investigation but has not met the required amount of time for purging shall be sent to the Records Division for storage.

4.2.1. Members shall send a summary of the different locations (e.g., ReJIN, LEDS, commercial databases) where information was found as well as any work product not available in an existing system (i.e., any work product created by the member as it pertains to the criminal case) to the Records Division.

4.3. Any criminal intelligence document or file exceeding the allotted retention timeframe may be purged by the original author, their supervisor or manager, or the Records Division. Members shall refer to Directive 1200.00, Inspections, Maintenance, Responsibility and Authority, for more information.

Provide feedback here.